Per la sicurezza non basta più un SMS

Di Andrew Showstead, Director of Technical Consultancy and Market Solutions - VASCO Data Security

Lo scorso luglio il *National Institute of Standards and Technology* (NIST), l'agenzia governativa degli Stati Uniti che si occupa della gestione delle tecnologie, ha finalmente dichiarato ciò che i professionisti della sicurezza, come anche gli hacker, già sapevano da anni: gli SMS non sono sicuri e non sono più adatti come meccanismo di strong authentication. I messaggi SMS non sono protetti da sguardi indiscreti e non c'è alcuna garanzia che essi giungano effettivamente al destinatario desiderato.
Quella del NIST è una conclusione annunciata: tutti sapevano che questo giorno sarebbe arrivato, eppure decine di applicazioni ricorrevano agli SMS come meccanismo di sicurezza. Come mai?

La risposta è piuttosto semplice: quando la gente ha cominciato a perdere fiducia nei servizi protetti da password, gli SMS hanno reso disponibile un processo economico, diffuso e facile da capire per poter dare agli utenti un senso di sicurezza. Nel migliore dei casi, gli SMS sono stati utilizzati per l'accesso a siti web a basso rischio; nel peggiore dei casi, per l'accesso a proprietà intellettuali rilevanti, a reti "sicure" e anche ad emittenti di carte di credito e istituzioni finanziarie. Con tecniche da "venditori ambulanti" privi di alternative adeguate, gli SMS venivano proposti con frasi ad effetto, quali autenticazione *out-of-band* e *step-up*. Ma la realtà, oggi, è che la sicurezza degli SMS non dà luogo a un vero e proprio "secondo fattore", come alcuni possono aver sostenuto; gli attacchi contro gli SMS non sono più teorici, ma diffusi.

Fin dall'inizio, gli SMS hanno sempre fornito un link "logico" tra il numero di telefono dell'utente e l'effettivo dispositivo che questi ha in mano. Prima di smartphone e app indispensabili, il punto di compromesso era l'account wireless dell'utente; una volta cambiato il telefono registrato a un account, il gioco era fatto: i messaggi venivano ricevuti senza che neanche si violasse l'account sotto attacco. In sostanza, si faceva affidamento sulle compagnie telefoniche per mantenere la sicurezza. In alcuni casi, i fornitori hanno aumentato la sicurezza associata a questo cambio di dispositivi, ritardando forse l'inevitabile.

Molti, ingenuamente, credono che l'unico modo che qualcuno ha di leggere i loro SMS è entrare in possesso del loro telefono e hanno un falso senso di maggior sicurezza se utilizzano un codice di accesso o l'impronta digitale per proteggerne l'accesso. È un grosso sbaglio, perché oggi come oggi c'è la concreta possibilità, per un malintenzionato, di attaccare direttamente il telefono. Un utente medio scarica ogni tipo di app, di solito concedendo permessi vari senza pensarci troppo, e spesso il download avviene da store non attendibili oppure utilizzando telefoni sottoposti a *jailbreaking* o a *rooting*: tutte situazioni che nascondono dei rischi.

Consideriamo la varietà di applicazioni disponibili per uso “legittimo”. Ad esempio, si desidera osservare i messaggi dei propri figli per sapere con chi socializzano? O aiutare un genitore anziano controllando gli SMS provenienti da uno dei vari servizi che potrebbe usare? Basta semplicemente installare un’utenza SMS nascosta sul loro telefono cellulare e vedere da remoto tutti i messaggi in entrata e in uscita. Se queste applicazioni esistono e possono agire in tal modo al nostro comando, perché un hacker non potrebbe utilizzarle nascondendole in un’app a nostra insaputa? Può accadere in diversi modi: riconfigurazione dell’applicazione, inserimento di codice, sovrapposizioni di schermo, tastiere corrotte.... Si sta scaricando l'ultima applicazione virale? Potrebbero arrivare anche un paio di gadget extra a cui non si è interessati, ma che probabilmente sono in grado di rubare credenziali di accesso.

Cosa fare quindi? Le alternative esistono e le applicazioni possono essere protette con sistemi di auto-protezione *run-time*, con una reale sicurezza delle transazioni o con tecnologie *device-binding*, consentendo ai cellulari di poter essere ancora utilizzati come un importante “secondo fattore”. Certamente, non ci si può più affidare agli SMS per la sicurezza.